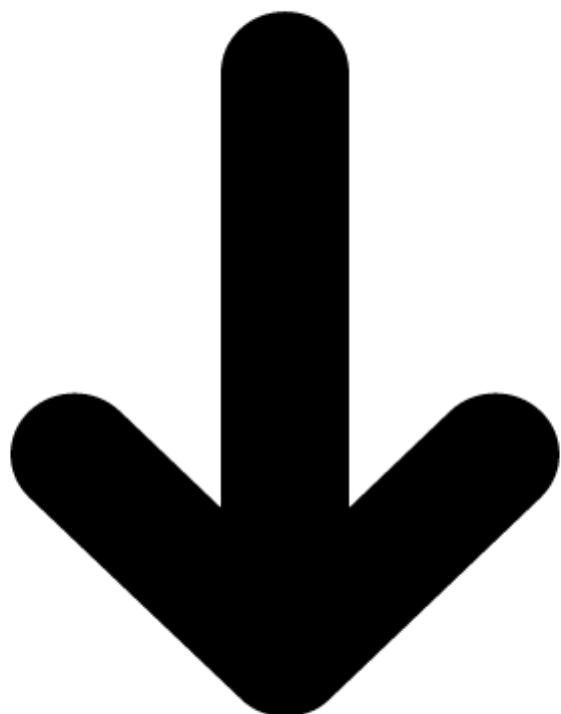


Proyek 6: Implementasi IDS (Intrusion Detection System) dengan Snort / Suricata

Nama Kelompok :

- 2201020098 Muhammad Rifqi
- 2201020123 Handicap
- 2201020139 Muhammad Iqbal Hordani
- 2201020101 Irsyad Widiansyah



Tahapan 3: Simulasi port scanning dengan nmap

- Port Scanning

Port scanning adalah teknik untuk memeriksa port-port yang terbuka pada suatu host atau server.

Tujuan scanning ini adalah untuk:

- mengidentifikasi layanan (service) yang berjalan,
- mengetahui port mana yang terbuka atau tertutup,
- memetakan potensi celah keamanan pada sistem.

Dalam konteks keamanan jaringan, port scan merupakan aktivitas yang sering dilakukan oleh penyerang (attacker) untuk mengumpulkan informasi sebelum melakukan serangan lebih lanjut. Oleh karena itu, Intrusion Detection System (IDS) seperti Suricata harus mampu mendeteksi pola scanning tersebut.

- Nmap

Nmap adalah singkatan dari **Network Mapper**, yaitu alat pemindai jaringan berbasis **opensource** yang digunakan untuk menemukan perangkat, port terbuka, dan layanan yang berjalan dalam suatu jaringan komputer. Nmap berfungsi untuk eksplorasi jaringan dan audit keamanan, serta membantu dalam mengidentifikasi potensi kerentanan dalam sistem jaringan. Alat ini sangat populer di kalangan profesional keamanan informasi dan digunakan untuk berbagai tujuan, termasuk pemetaan jaringan dan pengujian penetrasi.

- Tujuan Simulasi

1. Menghasilkan aktivitas port scanning dari mesin attacker menggunakan Nmap
2. Memvalidasi apakah Suricata dapat mendeteksi pola scan tersebut
3. Menghasilkan log yang dapat dianalisis pada tahap selanjutnya

Dengan melakukan simulasi ini, mahasiswa dapat memahami bagaimana IDS mendeteksi pola scanning melalui rule bawaan Suricata.

Progres

1. Install Nmap

- sudo apt update
- sudo apt install nmap

```
ubuntu@ubuntuserver:~$ sudo apt update
[sudo] password for ubuntu:
Get:1 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Hit:2 http://id.archive.ubuntu.com/ubuntu noble InRelease
Hit:3 http://id.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:4 http://id.archive.ubuntu.com/ubuntu noble-backports InRelease
Get:5 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [1,340 kB]
Hit:6 https://ppa.launchpadcontent.net/oisf/suricata-stable/ubuntu noble InRelease
Get:7 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [219 kB]
Get:8 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [21.5 kB]
Get:9 http://security.ubuntu.com/ubuntu noble-security/main amd64 c-n-f Metadata [9,452 B]
Get:10 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [2,194 kB]
Get:11 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [501 kB]
Get:12 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]
Get:13 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [915 kB]
Get:14 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [206 kB]
Get:15 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [71.5 kB]
Get:16 http://security.ubuntu.com/ubuntu noble-security/universe amd64 c-n-f Metadata [19.5 kB]
Get:17 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [212 B]
Fetched 5,623 kB in 8s (662 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
37 packages can be upgraded. Run 'apt list --upgradable' to see them.
ubuntu@ubuntuserver:~$ sudo apt install nmap
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libfdt1 libhttp2 libluajit-5.1-2 libnetfilter-log1 librte-bus-pci24 librte-bus-vdev24 librte-eal24 librte-ethdev24
  librte-hash24 librte-ip-frag24 librte-kvargs24 librte-log24 librte-mbuf24 librte-mempool24 librte-meter24
  librte-net-bond24 librte-net24 librte-pci24 librte-rcu24 librte-ring24 librte-sched24 librte-telemetry24 libxdp1
  oinkmaster snort-rules-default
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libblas3 liblinear4 liblua5.4-0 libssh2-1t64 nmap-common
Suggested packages:
  liblinear-tools liblinear-dev ncat zenmap
The following NEW packages will be installed:
  libblas3 liblinear4 liblua5.4-0 libssh2-1t64 nmap nmap-common
0 upgraded, 6 newly installed, 0 to remove and 37 not upgraded.
Need to get 6,452 kB of archives.
After this operation, 28.0 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://id.archive.ubuntu.com/ubuntu noble-updates/main amd64 libblas3 amd64 3.12.0-3build1.1 [238 kB]
Get:2 http://id.archive.ubuntu.com/ubuntu noble/universe amd64 liblinear4 amd64 2.3.0+dfsg-5build1 [42.3 kB]
Get:3 http://id.archive.ubuntu.com/ubuntu noble/main amd64 liblua5.4-0 amd64 5.4.6-3build2 [166 kB]
Get:4 http://id.archive.ubuntu.com/ubuntu noble/main amd64 libssh2-1t64 amd64 1.11.0-4.1build2 [120 kB]
Get:5 http://id.archive.ubuntu.com/ubuntu noble/universe amd64 nmap-common all 7.94+git20230807.3be01efb1+dfsg-3build2 [4,192 kB]
Get:6 http://id.archive.ubuntu.com/ubuntu noble/universe amd64 nmap amd64 7.94+git20230807.3be01efb1+dfsg-3build2 [1,694 kB]
Fetched 6,452 kB in 2s (3,212 kB/s)
Selecting previously unselected package libblas3:amd64.
(Reading database ... 88467 files and directories currently installed.)
```

- cek instalasi Nmap : nmap -v

```
ubuntu@ubuntuserver:~$ nmap -v
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-28 07:40 UTC
Read data files from: /usr/bin/../share/nmap
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.02 seconds
```

2. Simulasi Port Scanning dengan Nmap, Ip target = 192.168.56.102

- Normal scan

Normal scan adalah metode scanning standar Nmap yang digunakan untuk memeriksa port mana saja yang terbuka pada target. Scan ini mengirimkan paket TCP ke beberapa port umum dan menampilkan status port seperti **open**, **closed**, atau **filtered**.

Perintah : nmap <IP_Target>

```
ubuntu@ubuntuserver:~$ nmap 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-28 07:52 UTC
Nmap scan report for 192.168.56.102 (192.168.56.102)
Host is up (0.000045s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
```

Output :

- **Host is up** → Artinya IP tersebut aktif dan bisa dijangkau.
- **Not shown: 999 closed ports** → Ada 999 port yang tertutup.
- **22/tcp open ssh** → Port 22 (SSH) terbuka.

- SYN scan (Stealth Scan)

SYN scan adalah jenis scanning yang hanya mengirim paket **SYN** tanpa menyelesaikan proses handshake TCP. Teknik ini sering digunakan penyerang karena lebih cepat, lebih “diam-diam”, dan sering tidak tercatat oleh service target. IDS seperti Suricata biasanya mendeteksi scan ini sebagai aktivitas mencurigakan.

Perintah : sudo nmap -sS <IP_Target>

```
ubuntu@ubuntuserver:~$ sudo nmap -sS 192.168.56.102
[sudo] password for ubuntu:
Sorry, try again.
[sudo] password for ubuntu:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-28 07:56 UTC
Nmap scan report for 192.168.56.102 (192.168.56.102)
Host is up (0.0000060s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
```

Output :

- **Host is up** → Target aktif.
- **Not shown: 999 closed tcp ports (reset)** → Artinya 999 port mengirimkan respon **RST**, menunjukkan port tertutup.
- **22/tcp open ssh** → Port 22 terdeteksi **open**.

- Aggressive scan (-A Scan)

Aggressive scan melakukan scanning yang lebih lengkap:

- mendeteksi versi service
- identifikasi sistem operasi (OS detection)
- melakukan traceroute
- scanning port secara menyeluruh

Metode ini menghasilkan traffic lebih banyak dan mudah terdeteksi oleh IDS.

Perintah : sudo nmap -A <IP_Target>

```
ubuntu@ubuntuserver:~$ sudo nmap -A 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-11-28 07:59 UTC
Nmap scan report for 192.168.56.102 (192.168.56.102)
Host is up (0.000038s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.14 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 c4:4c:c7:1d:ba:9c:c7:fb:d6:a4:2f:0e:85:08:06:9c (ECDSA)
|_  256 f3:b9:a4:4c:bb:af:9d:97:0f:03:ae:21:69:e9:43:6f (ED25519)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.32
OS details: Linux 2.6.32
Network Distance: 0 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.93 seconds
ubuntu@ubuntuserver:~$ |
```

Output :

- **Target IP:** 192.168.56.102
- **Host Status:** Up
- **Port Terbuka:**
 - 22/tcp – OpenSSH 9.6p1 (Ubuntu)
- **SSH Host Key:**
 - Terdeteksi fingerprint ECDSA & ED25519
- **OS Detection:**
 - Sistem operasi teridentifikasi sebagai **Linux kernel 2.6.x**
- **Device Type:**
 - General purpose (mesin komputer umum)
- **Network Distance:** 0 hops (satu jaringan / langsung)
- **Waktu Scan:** ~1.93 detik